National Computer Board

CERT-MU

RFC 2350

1. Document Information

1.1. Date of Last Update

This is version 1.0 published 30-09-2020

1.2. Distribution List for Notifications

CERT-MU will not plan frequent modifications to this document.

1.3. Locations where this Document May Be Found

http://cert-mu.govmu.org/English/Documents/RFC%202350/RFC%202350.pdf

2. Contact Information

2.1. Name of the Team

CERT-MU, Computer Emergency Response Team of Mauritius

(National CERT of Mauritius)

2.2. Address

2nd Floor Wing A,Shri Atal Bihari Vajpayee Tower, Ebène Cybercity,

Mauritius

2.3. Time Zone

We are located in the Indian Ocean which is

- GMT+4, between last Sunday in October and last Sunday in March
- GMT+3, between last Sunday in March and last Sunday in October

2.4. Telephone Number

Tel: +230 2105520

Hotline: +230 8002378

2.5. Electronic Mail Address

contact@cert.ncb.mu – for general information

incident@cert.ncb.mu – for incident related matters

vulnerability@cert.ncb.mu – for reporting vulnerabilities

2.6. Public Keys and Encryption Information

1) Email: incident@cert.ncb.mu

   Fingerprint: B5C1F48C419AA042C741FD93C83FD88189FDAA7A

2) Email: contact@cert.ncb.mu

   Fingerprint:0497B41CAC2E6BF5179F81E3F01A4833D6FAED16

3) Email: certadvisory@cert.ncb.mu

   Fingerprint:7C8394810D1E8D62778E66263896F616D8DD722A

The public keys can be found at

https://cert-mu.govmu.org/Pages/PGP-Public-Key-Block.aspx

2.7. Team Members

The head of CERT-MU is Dr Kaleem Ahmed Usmani

Information about other team members is available upon request.

2.8. Other Information

- General information about CERT-MU is available at

http://cert-mu.govmu.org/English/Pages/default.aspx

- Online system for reporting cybercrimes

  http://maucors.govmu.org/English/Pages/default.aspx

2.9. Points of Customer Contact

The preferred communication channel is the telephone. If it is not possible to contact the CERT-MU by using the telephone, then please use the official email addresses as mentioned in section 2.5.

3. Charter

3.1. Mission Statement

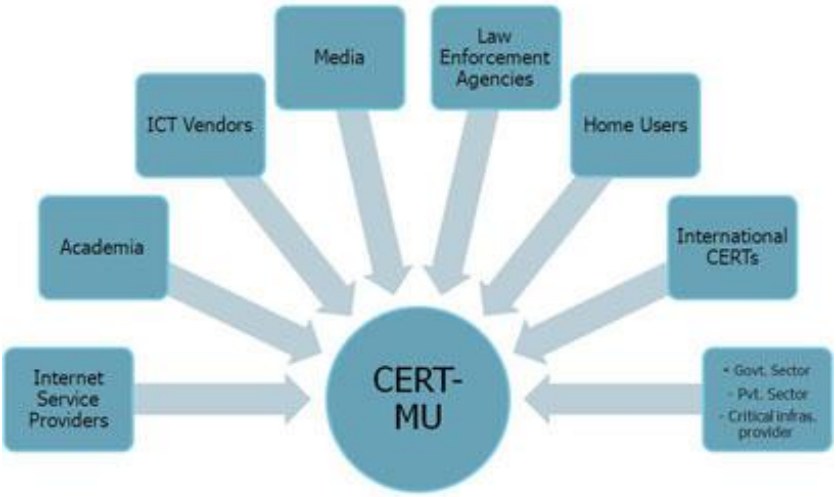
The main goals for CERT-MU as the national CERT are:

- Handle security incidents and monitor security problems occurring within public and private sectors.
- Provide guidance to providers of critical information infrastructure to adopt best practices in information security.
- Warn and educate systems administrators and users about latest information security threats and suggest countermeasures by means of information dissemination.

3.2. Constituency

CERT-MU's constituency will be as follows: -

- CERT-MU's constituency will be the entire cyber community of Mauritius.
- CERT-MU will receive intrusions attempts reports, virus incidents and other security problems from defined staff of each constituent within each institution, namely Security Contact Person(s).



3.3. Sponsorship and/or Affiliation

CERT-MU is a department of the National Computer Board which operates under the aegis of the Ministry of Information Technology, Communication and Innovation. CERT-MU is certified ISO 27001 since May 2017.

CERT-MU is a

- Member of Cybersecurity Alliance for Mutual Progress (CAMP)
- Member of Forum of Incident Response and Security Teams (FIRST)
- Member of Anti-Phishing Working Group (APWG)
- Member of Software Engineering Institute (SEI)
- Member of AfricaCERT

CERT-MU has also signed a memorandum of understanding (MoU) with CERT-IN

3.4 Authority

CERT-MU operates under the auspices of National Computer Board. As such, its authority is that given by NCB's Acceptable Use Policy (AUP), which is part of CERT-MU General Conditions.

4. Policies

4.1. Types of Incidents and Level of Support

CERT-MU is authorized to address all types of computer security incidents which occur, or threaten to occur, in its constituency. The level of support given by CERT-MU will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the CERT-MU's resources at the time. CERT-MU will

provide cooperation as soon as possible and will also provide support to its constituents. CERT-MU is also committed to keep all its constituents informed on potential vulnerabilities, and assistance to its constituents in implementing proactive measures to reduce the risks of information security incidents as well as responding to such incidents as and when they occur.

4.2. Co-operation, Interaction and Disclosure of Information

CERT-MU works in cooperation with State Institutions, Law Enforcement Organisations and professionals in the field. Standard privacy laws apply. In case of a potential criminal incident, we recommend the proper law enforcement organisations assistance. Rules and good practice are in place to avoid dissemination of private and company data.

4.3. Communication and Authentication

For international communications ordinary precautions apply – like communicating to/via previously trusted and listed teams (TI) and using PGP.

5. Services

5.1 Incident Response

CERT-MU will assist IT-security teams in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

- Investigating whether an incident is authentic
- Assessing and prioritizing the incident

5.1.2. Incident Coordination

- Determining and contacting the involved organisations.
- Facilitating contact with other parties including law enforcement, if needed.
- Asking for reports and/or composing reports, depending on the involved organisations, incident type and severity.
- Communicating with media, if necessary.

5.1.3. Incident Resolution

- Advising the involved organisation(s) on appropriate measures.
- Following up the incident solution process.
- Collecting evidence and interpreting data, if applicable.

CERT-MU will also collect statistics about incidents within its constituency.

5.2 Proactive Activities

- Issuance of Security Alerts
  - ❖ Website
  - ❖ Mailing Lists
  - ❖ Targeted alerts to critical sectors
- Organisation of Security Awareness Programmes
  - ❖ Organizing Trainings/workshops for CIOs and System administrators
  - ❖ Security awareness campaign for home users
- Collaboration with Industry and International CERTs
- Assistance to Organisations in the implementation of Information Security Management Systems (ISMS) based on ISO 27001 standard.
- Provide Vulnerability Scanning Service
- Provide Assistance as a third Party Auditor of Information Security Management Systems(ISMS) based on ISO 27001 standard

6. Incident Reporting Forms

- Incidents should be reported on the Mauritian Cybercrime Online Reporting System (MAUCORS) which is an online platform that allows the public to report cybercrimes
- Incidents can also be reported on email address incident@cert.ncb.mu and as well as at CERT-MU's office. For proof of identity, the incident reporting party should bring their Identity Card. An incident must be reported by the victim only or in case the person may not be able to come personally, then he/she can authorize any other, together with an authorization letter duly signed and ID card or power of attorney.

  Enquiries about incidents can be made through CERT-MU Hotline: **800 2378**

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-MU assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.